

 **Werise** @We_Have_Risen
7 Nov • 15 tweets • [We_Have_Risen/status/1325129915709104129](#) Tr

Good morning Dominion...

You ready to get your ass handed to you?

 **Werise**
@We_Have_Risen



Thank you 15...

In light of this video, which mirrors what happened in VA, let's look at a few things shall we...



BLOOMFIELD HILLS, MI
LIVE | WJBK 12:31 PM ET

KEY STATES

STATE	VOTE DIFFERENCE
ARIZONA	+43,779
GEORGIA	+1,584
NEVADA	+20,542
N. CAROLINA	+76,701
PENNSYLVANIA	+9,854

FOX BUSINESS
LIVE

MI GOP CHAIR GIVES UPDATE ON ELECTION

DOW
28,321.39
-68.79
-0.24%

Informed by You™

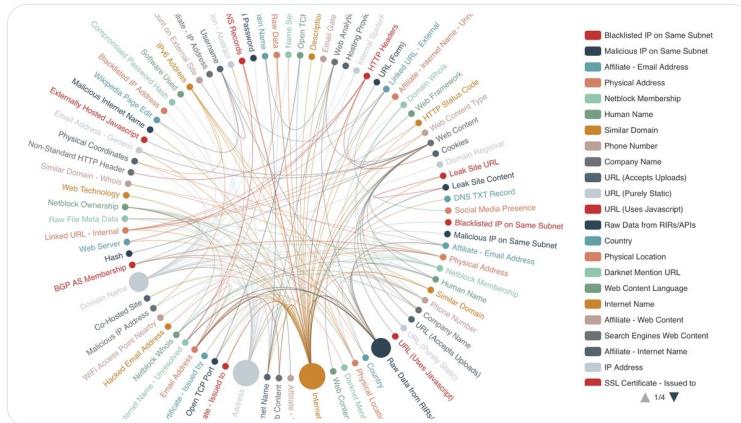
NAS 11,868.13 ▼ 22.79 -0.19% **RUSS 2K** 1,650.64 ▼ 9.41 -0.57%
D R

 **OnBreak** @15poundstogo

I would strongly suggest following @We_Have_Risen
If we're gonna see any serious evidence of large-scale ghost voting, or not, that's where to look. [twitter.com/We_Have_Risen/...](https://twitter.com/We_Have_Risen/)

11:42 PM · Nov 6, 2020

 2.8K  1.9K people are Tweeting about this



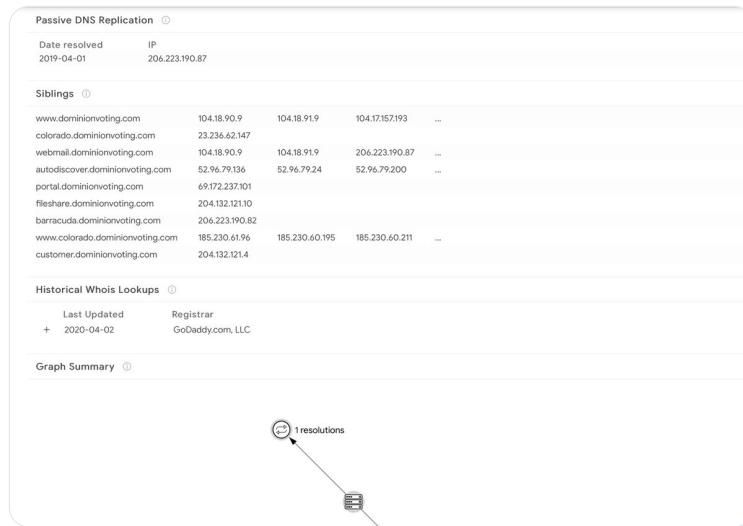
We have quite a bit to work with overnight...

No honor amongst thieves...

You have something to say I suggest you say it now. You will be exposed and we will hunt every last one...

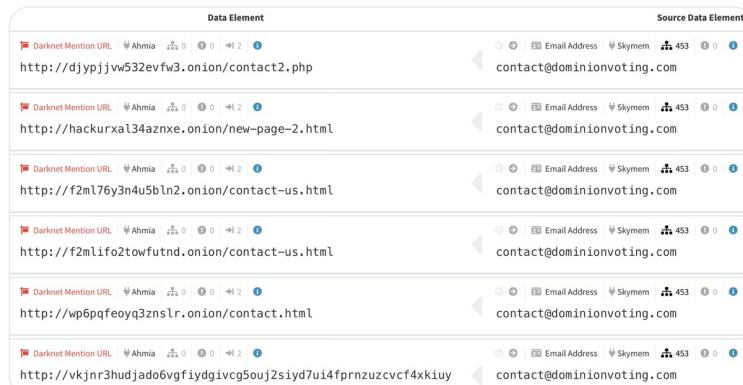


Care to explain why you are blacklisted and show up on the Threat Intel sites 75+ times 🤪



Ahhhhh, that explains it...

Makes me feel so much better you are all over the Dark Web...



That's cool can you make sure that Cloudflare only blocks the transmission of [@realDonaldTrump](#) votes? K thanks

Data Element	Source Data Element
Malicious Internet Name CloudFlare Malware DNS Blocked by CloudFlare DNS [selector2._domainkey.dominionvoting.com]	Internet Name RiskIQ selector2._domainkey.dominionvoting.com
Malicious Internet Name CloudFlare Malware DNS Blocked by CloudFlare DNS [selector1._domainkey.dominionvoting.com]	Internet Name RiskIQ selector1._domainkey.dominionvoting.com

Making more and more sense...

Honeypot for who though?

The screenshot shows a honeypot tracker interface for the IP address 23.236.62.147. The details page includes:

- Data Type:** Malicious IP Address
- Starred:** No
- Source Module(s):** Fraudguard
- Raw Data:** honeypot_tracker (risk level: 5) [23.236.62.147]
- Risky Data Type?:** Yes
- Data Source(s):** Fraudguard
- Status Description:** Fraudguard

Hi

The screenshot shows a summary page for the 'Leak-Lookup' module with the filter 'Risky: Yes'. There are 9 results listed:

- steven.bennett@dominionvoting.com [verifications.io]
- steven.bennett@dominionvoting.com [evite.com]
- steven.bennett@dominionvoting.com [linkedin.com]
- kay.stimson@dominionvoting.com [apollo.io]
- jim.alexander@dominionvoting.com [verifications.io]
- nakia.brown@dominionvoting.com [apollo.io]

Each result row contains a 'Hacked Email Address' icon, a 'Leak-Lookup' icon, a status bar (0/0), and an information icon.

That's cool because those httpd's are secure right?

Data Element							
 Software Used	 SHODAN	 0	 0	 3			
Microsoft Exchange smtpd							
 Software Used	 SHODAN	 0	 0	 3			
Rhinosoft Serv-U httpd							
 Software Used	 SHODAN	 0	 0	 3			
Microsoft IIS httpd							
 Software Used	 SHODAN	 0	 0	 3			
Microsoft IIS httpd							
 Software Used	 SHODAN	 0	 0	 3			
Microsoft IIS httpd							
 Software Used	 SHODAN	 0	 0	 3			
Microsoft IIS httpd							

I have captured quite a bit the last couple of days. Shoot me what you got and I will do the same 🤘



John
@Johnheretohelp

Replying to @Johnheretohelp

And porn sites. There was access through the USPS.
One odd thing.
Dominion WAS NOT HACKED as far as I can tell now. They had access to it already, they just approached it from multiple directions to hide their activity.
These weren't "glitches" 🤦‍♂️🤦‍♂️

4:12 PM · Nov 7, 2020



 2.8K  1.6K people are Tweeting about this

Porn sites like this one 😅



Wow these people are comp'd af...

I haven't really even dug in yet but it is a joke how bad it is...

Module Category	Risky	Unique
Content Analysis	0	1841
Crawling and Scanning	0	845
DNS	29	277
Internal	0	3
Leaks, Dumps and Breaches	36	39
Passive DNS	0	884
Public Registries	0	47
Real World	0	102
Reputation Systems	347	1159
Search Engines	492	1130
Secondary Networks	0	577
Social Media	0	48



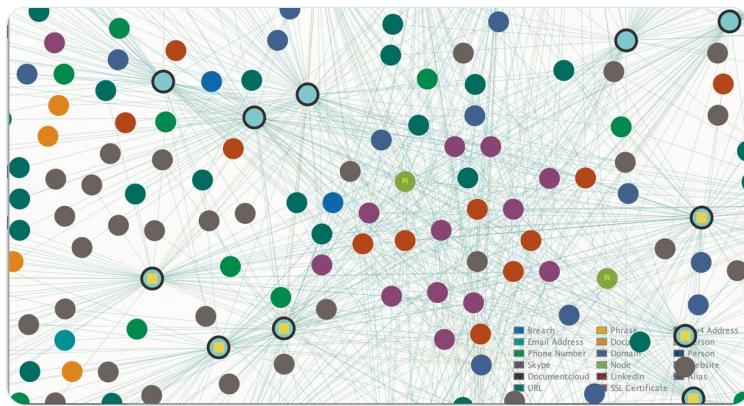
Summary > Module Category: Leaks, Dumps and Breaches (1 - 100 out of 1237 results)

Data Element	Source Data Element
Compromised Password Scylla 0 0 41 phil.foster@dominionvoting.com:Odie1218 [Collections]	Domain Name SpiderFoot UI 133 dominionvoting.com
Compromised Password Scylla 0 0 41 jack.blaine@dominionvoting.com:Bruins69 [avvo.com]	Domain Name SpiderFoot UI 133 dominionvoting.com
Compromised Password Scylla 0 0 41 joe.mcintyre@dominionvoting.com:peanut00 [Collections]	Domain Name SpiderFoot UI 133 dominionvoting.com
Compromised Password Scylla 0 0 41 joe.mcintyre@dominionvoting.com:Peanut00 [Collections]	Domain Name SpiderFoot UI 133 dominionvoting.com
Compromised Password Scylla 0 0 41 jelena.tanaskovic@dominionvoting.com:dzigibau [Collections]	Domain Name SpiderFoot UI 133 dominionvoting.com
Compromised Password Scylla 0 0 41 christina.reich@dominionvoting.com:6V21wbgad [Collection1-btc-]	Domain Name SpiderFoot UI 133 dominionvoting.com

Occasional travel “both” domestic...



What a tangled web we weave...

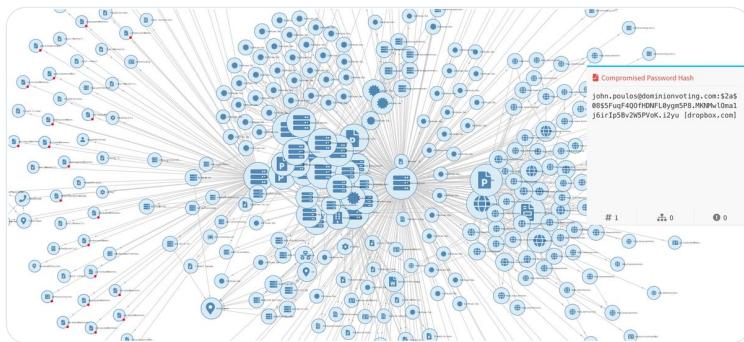


Everyone...

Let's look at the election security laws/guidance by state...

GA blaming the “glitch” on a software update is their biggest mistake as the machines are not supposed to be connected...

We know they are and they admitted it...



...